Notice of Allowability	Application No.	Applicant(s)	
	09/931,803	SCHON ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *5/31/2006*.

2. ☒ The allowed claim(s) is/are *1,3,5-7,10,12,14-16,19,20,22-24,26,28-30,32,33,35-37,39,42,43,45,46,48,51,53,56-58,60,61,63-65,67 and 70*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *6/26/2006* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 5/31/2006 has been entered.

Examiner's Amendment

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Kevin J. Zilka (Reg. No. 41,429) on 6/26/2006.

This application has been amended as follows:

IN THE CLAIMS

Cancel claim 2, 4, 8, 9, 11, 13, 17, 18, 21, 25, 27, 31, 34, 38, 40, 41, 44, 47, 49, 50, 52, 54, 55, 59, 62, 66 and 68 – 69 without prejudice.

Replace claim 1, 10, 20, 26, 33, 39, 46, 51, 57, 60, 64 and 67 as follows.

Claim 1: A system for automatically protecting private video content using embedded cryptographic security, comprising:

a recorder frame buffer dividing a substantially continuous video signal representing raw video content into individual frames which each store a fixed amount of data in digital form;

an encryption module encrypting each individual frame into encrypted video content using an encryption cryptographic key and storing the encrypted frames on a transportable storage medium;

a decryption module retrieving encrypted frames from the transportable storage medium and decrypting each encrypted frame into decrypted frames using a decryption cryptographic key that is verified prior to decryption;

a playback frame buffer combining the decrypted frames into a substantially continuous video signal representing the raw video content in reconstructed form;

a signature module generating a fixed-length original cryptographic hash from at least one such individual frame, encrypting the original cryptographic hash using an encryption cryptographic key, and storing the encrypted original cryptographic hash as a digital signature on the transportable storage medium;

a verification module retrieving the digital signature from the transportable storage medium, decrypting the encrypted original cryptographic hash using a decryption cryptographic key, generating a verification fixed-length cryptographic hash from at least one such corresponding decrypted frame, and comparing the verification cryptographic hash and the original cryptographic hash;

~~a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key such that a plurality of encryption cryptographic keys, each associated with a different removable storage medium, are capable of being utilized for encrypting the individual frames;~~

a validation module validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames; [[and]]

a set of cryptographic instructions [[stored on the removable storage medium and]] employing at least one of the encryption cryptographic key and the decryption cryptographic key; and

a removable storage medium storing at least one of the encryption cryptographic key or the decryption cryptographic key such that a plurality of encryption or decryption cryptographic keys, associated with the removable storage medium, are capable of being utilized for encrypting or decrypting the individual frames, wherein the removable storage medium comprises only memory that stores the set of cryptographic instructions and the plurality of the encryption or decryption cryptographic keys, and is separate from a player which is capable of playing the video content on the transportable storage medium or a recorder which is capable of recording the video content on the transportable storage medium;

wherein only encrypted and signed video content passes a first physical boundary separating [[a]]the recorder from the transportable storage medium;

wherein only the encrypted and signed video content passes a second physical boundary separating the transportable storage medium from [[a]]the player;

~~wherein only signed video content passes the first physical boundary separating the recorder from the transportable storage medium;~~

~~wherein only the signed video content passes the second physical boundary separating the transportable storage medium from the player~~.

Claim 10: A method for automatically protecting private video content using embedded cryptographic security, comprising:

dividing a substantially continuous video signal representing raw video content into individual frames which each store a fixed amount of data in digital form;

encrypting each individual frame into encrypted video content using an encryption cryptographic key and storing the encrypted frames on a transportable storage medium;

retrieving encrypted frames from the transportable storage medium and decrypting each encrypted frame into decrypted frames using a decryption cryptographic key that is verified prior to decryption;

combining the decrypted frames into a substantially continuous video signal representing the raw video content in reconstructed form;

generating a fixed-length original cryptographic hash from at least one such individual frame;

encrypting the original cryptographic hash using an encryption cryptographic key and storing the encrypted original cryptographic hash as a digital signature on the transportable storage medium;

retrieving the digital signature from the transportable storage medium and decrypting the encrypted original cryptographic hash using a decryption cryptographic key;

generating a verification fixed-length cryptographic hash from at least one such corresponding decrypted frame and comparing the verification cryptographic hash and the original cryptographic hash;

~~providing at least one of the encryption cryptographic key and the decryption cryptographic key on a removable storage medium such that a plurality of encryption cryptographic keys, each associated with a different removable storage medium, are capable of being utilized for encrypting the individual frames;~~

validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames; [[and]]

including a set of cryptographic instructions employing at least one of the encryption cryptographic key and the decryption cryptographic key[[on the removable storage medium]]; and

storing on a removable storage medium at least one of the encryption cryptographic key or the decryption cryptographic key such that a plurality of encryption or decryption cryptographic keys, associated with the removable storage medium, are capable of being utilized for encrypting or decrypting the individual frames, wherein the removable storage medium comprises only memory that stores the set of cryptographic

instructions and the plurality of the encryption or decryption cryptographic keys, and is separate from a player which is capable of playing the video content on the transportable storage medium or a recorder which is capable of recording the video content on the transportable storage medium;

wherein only encrypted and signed video content passes a first physical boundary separating [[a]]the recorder from the transportable storage medium;

wherein only the encrypted and signed video content passes a second physical boundary separating the transportable storage medium from [[a]]the player;

~~wherein only signed video content passes the first physical boundary separating the recorder from the transportable storage medium;~~

~~wherein only the signed video content passes the second physical boundary separating the transportable storage medium from the player~~.

Claim 19: A computer-readable storage medium holding code for performing the method according to Claims 10, 12, ~~13~~, 14, 15 or 16.

Claim 20: A system for encrypting private video content using embedded cryptographic security, comprising:

a frame buffer receiving a substantially continuous video signal representing raw video content and dividing the data signal into individual frames which each store a fixed amount of data in digital form;

a processor encrypting each individual frame into encrypted video content using an encryption cryptographic key selected from a cryptographic key pair; and

a recorder storing the encrypted frames on a transportable storage medium for retrieval and decryption using a decryption cryptographic key selected from the cryptographic key pair,

wherein the processor generates a fixed-length original cryptographic hash from at least one such individual frame and encrypts the original cryptographic hash using an

encryption cryptographic key selected from the cryptographic key pair and the recorder stores the encrypted original cryptographic hash as a digital signature on the transportable storage medium for retrieval and verification using a decryption cryptographic key selected from the cryptographic key pair,

~~wherein at least one of the encryption cryptographic key and the decryption cryptographic key is stored on a removable storage medium such that a plurality of encryption cryptographic keys, each associated with a different removable storage medium, are capable of being utilized for encrypting the individual frames;~~

wherein the decryption cryptographic key is validated against user-provided credentials prior to decrypting the encrypted frames;

wherein a set of cryptographic instructions [[is stored on the removable storage medium and]] employs at least one of the encryption cryptographic key and the decryption cryptographic key;

wherein a removable storage medium stores at least one of the encryption cryptographic key or the decryption cryptographic key such that a plurality of encryption or decryption cryptographic keys, associated with the removable storage medium, are capable of being utilized for encrypting or decrypting the individual frames, where the removable storage medium comprises only memory that stores the set of cryptographic instructions and the plurality of the encryption or decryption cryptographic keys, and is separate from a player which is capable of playing the video content on the transportable storage medium or the recorder which is capable of recording the video content on the transportable storage medium;

wherein only encrypted and signed video content passes a first physical boundary separating [[a]]the recorder from the transportable storage medium;

wherein only the encrypted and signed video content passes a second physical boundary separating the transportable storage medium from [[a]]the player;

~~wherein only signed video content passes the first physical boundary separating the recorder from the transportable storage medium;~~

~~wherein only the signed video content passes the second physical boundary separating the transportable storage medium from the player~~.

Claim 26: A method for encrypting private video content using embedded cryptographic security, comprising:

receiving a substantially continuous video signal representing raw video content and dividing the data signal into individual frames which each store a fixed amount of data in digital form;

encrypting each individual frame into encrypted video content using an encryption cryptographic key selected from a cryptographic key pair;

storing the encrypted frames on a transportable storage medium for retrieval and decryption using a decryption cryptographic key selected from the cryptographic key pair;

generating a fixed-length original cryptographic hash from at least one such individual frame;

encrypting the original cryptographic hash using an encryption cryptographic key selected from the cryptographic key pair;

storing the encrypted original cryptographic hash as a digital signature on the transportable storage medium for retrieval and verification using a decryption cryptographic key selected from the cryptographic key pair;

~~providing at least one of the encryption cryptographic key and the decryption cryptographic key on a removable storage medium such that a plurality of encryption cryptographic keys, each associated with a different removable storage medium, are capable of being utilized for encrypting the individual frames;~~

validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames; [[and]]

including a set of cryptographic instructions employing at least one of the encryption cryptographic key and the decryption cryptographic key[[on the removable storage medium]]; and

storing in a removable storage medium at least one of the encryption cryptographic key or the decryption cryptographic key such that a plurality of encryption or decryption cryptographic keys, associated with the removable storage medium, are capable of being utilized for encrypting or decrypting the individual frames, wherein the

removable storage medium comprises only memory that stores the set of cryptographic instructions and the plurality of the encryption or decryption cryptographic keys, and is separate from a player which is capable of playing the video content on the transportable storage medium or a recorder which is capable of recording the video content on the transportable storage medium;

wherein only encrypted and signed video content passes a first physical boundary separating [[a]]the recorder from the transportable storage medium;

wherein only the encrypted and signed video content passes a second physical boundary separating the transportable storage medium from [[a]]the player;

~~wherein only signed video content passes the first physical boundary separating the recorder from the transportable storage medium;~~

~~wherein only the signed video content passes the second physical boundary separating the transportable storage medium from the player~~.

Claim 33: A system for decrypting private video content using embedded cryptographic security, comprising:

a player retrieving encrypted frames from a transportable storage medium, the encrypted frames storing raw video content encrypted using an encryption cryptographic key selected from a cryptographic key pair;

a processor decrypting each encrypted frame using a decryption cryptographic key selected from the cryptographic key pair; and

a frame buffer combining the decrypted frames into a substantially continuous video signal representing the raw video content in reconstructed form,

wherein the player retrieves a digital signature from the transportable storage medium, the digital signature containing an original cryptographic hash encrypted using an encryption cryptographic key selected from the cryptographic key pair, and the processor decrypts the encrypted original cryptographic hash using a decryption cryptographic key selected from the cryptographic key pair, generates a verification fixed-length cryptographic hash from at least one individual frame retrieved from the

transportable storage medium, and compares the verification cryptographic hash and the original cryptographic hash; [[and]]

~~a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key such that a plurality of encryption cryptographic keys, each associated with a different removable storage medium, are capable of being utilized for encrypting the individual frames;~~

wherein the decryption cryptographic key is validated against user-provided credentials prior to decrypting the encrypted frames;

wherein a set of cryptographic instructions [[is stored on the removable storage medium and]]employs at least one of the encryption cryptographic key and the decryption cryptographic key;

wherein a removable storage medium stores at least one of the encryption cryptographic key or the decryption cryptographic key such that a plurality of encryption or decryption cryptographic keys, associated with the removable storage medium, are capable of being utilized for encrypting or decrypting the individual frames, where the removable storage medium comprises only memory that stores the set of cryptographic instructions and the plurality of the encryption or decryption cryptographic keys, and is separate from a player which is capable of playing the video content on the transportable storage medium or a recorder which is capable of recording the video content on the transportable storage medium;

wherein only encrypted and signed video content passes a first physical boundary separating [[a]]the recorder from the transportable storage medium;

wherein only the encrypted and signed video content passes a second physical boundary separating the transportable storage medium from [[a]]the player;

~~wherein only signed video content passes the first physical boundary separating the recorder from the transportable storage medium;~~

~~wherein only the signed video content passes the second physical boundary separating the transportable storage medium from the player~~.

Claim 39: A method for decrypting private video content using embedded cryptographic security, comprising:

retrieving encrypted frames from a transportable storage medium, the encrypted frames storing raw video content encrypted using an encryption cryptographic key selected from a cryptographic key pair;

decrypting each encrypted frame using a decryption cryptographic key selected from the cryptographic key pair;

combining the decrypted frames into a substantially continuous video signal representing the raw video content in reconstructed form;

retrieving a digital signature from the transportable storage medium, the digital signature containing an original cryptographic hash encrypted using an encryption cryptographic key selected from the cryptographic key pair;

decrypting the encrypted original cryptographic hash using a decryption cryptographic key selected from the cryptographic key pair;

generating a verification fixed-length cryptographic hash from at least one individual frame retrieved from the transportable storage medium and comparing the verification cryptographic hash and the original cryptographic hash;

~~providing at least one of the encryption cryptographic key and the decryption cryptographic key on a removable storage medium such that a plurality of encryption cryptographic keys, each associated with a different removable storage medium, are capable of being utilized for encrypting the individual frames;~~

validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames; [[and]]

including a set of cryptographic instructions employing at least one of the encryption cryptographic key and the decryption cryptographic key[[on the removable storage medium]]; and

storing on a removable storage medium at least one of the encryption cryptographic key or the decryption cryptographic key such that a plurality of encryption or decryption cryptographic keys, associated with the removable storage medium, are capable of being utilized for encrypting or decrypting the individual frames, wherein the

removable storage medium comprises only memory that stores the set of cryptographic instructions and the plurality of the encryption or decryption cryptographic keys, and is separate from a player which is capable of playing the video content on the transportable storage medium or a recorder which is capable of recording the video content on the transportable storage medium;

wherein only encrypted and signed video content passes a first physical boundary separating [[a]]the recorder from the transportable storage medium;

wherein only the encrypted and signed video content passes a second physical boundary separating the transportable storage medium from [[a]]the player;

~~wherein only signed video content passes the first physical boundary separating the recorder from the transportable storage medium;~~

~~wherein only the signed video content passes the second physical boundary separating the transportable storage medium from the player~~.

Claim 46: A system for automatically authenticating private video content using embedded cryptographic security, comprising:

a recorder frame buffer dividing a substantially continuous video signal representing raw video content into individual frames which each store a fixed amount of data in digital form;

a signature module generating a fixed-length original cryptographic hash from at least one such individual frame, encrypting the original cryptographic hash using an encryption cryptographic key comprising a private key of an asymmetric cryptographic pair, and storing the encrypted original cryptographic hash as a digital signature on a transportable storage medium;

a verification module retrieving the digital signature from the transportable storage medium and decrypting the encrypted original cryptographic hash using a decryption cryptographic key comprising a public key of an asymmetric cryptographic pair;

a player frame buffer generating a verification fixed-length cryptographic hash from at least one such individual frame and comparing the verification cryptographic hash and the original cryptographic hash;

~~a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key such that a plurality of encryption cryptographic keys, each associated with a different removable storage medium, are capable of being utilized for encrypting the individual frames;~~

a validation module validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames; [[and]]

a set of cryptographic instructions [[stored on the removable storage medium and]]employing at least one of the encryption cryptographic key and the decryption cryptographic key; and

a removable storage medium storing at least one of the encryption cryptographic key or the decryption cryptographic key such that a plurality of encryption or decryption cryptographic keys, associated with the removable storage medium, are capable of being utilized for encrypting or decrypting the individual frames, wherein the removable storage medium comprises only memory that stores the set of cryptographic instructions and the plurality of the encryption or decryption cryptographic keys, and is separate from a player which is capable of playing the video content on the transportable storage medium or a recorder which is capable of recording the video content on the transportable storage medium;

wherein only encrypted and signed video content passes a first physical boundary separating [[a]]the recorder from the transportable storage medium;

wherein only the encrypted and signed video content passes a second physical boundary separating the transportable storage medium from [[a]]the player;

~~wherein only signed video content passes the first physical boundary separating the recorder from the transportable storage medium;~~

~~wherein only the signed video content passes the second physical boundary separating the transportable storage medium from the player~~.

Claim 51: A method for automatically authenticating private video content using embedded cryptographic security, comprising:

dividing a substantially continuous video signal representing raw video content into individual frames which each store a fixed amount of data in digital form and generating a fixed-length original cryptographic hash from at least one such individual frame;

encrypting the original cryptographic hash using an encryption cryptographic key comprising a private key of an asymmetric cryptographic pair and storing the encrypted original cryptographic hash as a digital signature on a transportable storage medium;

retrieving the digital signature from the transportable storage medium and decrypting the encrypted original cryptographic hash using a decryption cryptographic key comprising a public key of an asymmetric cryptographic pair;

generating a verification fixed-length cryptographic hash from at least one such individual frame and comparing the verification cryptographic hash and the original cryptographic hash;

~~providing at least one of the encryption cryptographic key and the decryption cryptographic key on a removable storage medium such that a plurality of encryption cryptographic keys, each associated with a different removable storage medium, are capable of being utilized for encrypting the individual frames;~~

validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames; [[and]]

including a set of cryptographic instructions employing at least one of the encryption cryptographic key and the decryption cryptographic key[[on the removable storage medium]]; and

storing on a removable storage medium at least one of the encryption cryptographic key or the decryption cryptographic key such that a plurality of encryption or decryption cryptographic keys, associated with the removable storage medium, are capable of being utilized for encrypting or decrypting the individual frames, wherein the removable storage medium comprises only memory that stores the set of cryptographic instructions and the plurality of the encryption or decryption cryptographic keys, and is

separate from a player which is capable of playing the video content on the transportable storage medium or a recorder which is capable of recording the video content on the transportable storage medium;

wherein only encrypted and signed video content passes a first physical boundary separating [[a]]the recorder from the transportable storage medium;

wherein only the encrypted and signed video content passes a second physical boundary separating the transportable storage medium from [[a]]the player;

~~wherein only signed video content passes the first physical boundary separating the recorder from the transportable storage medium;~~

~~wherein only the signed video content passes the second physical boundary separating the transportable storage medium from the player~~.

Claim 57: A system for digitally signing private video content using embedded cryptographic security, comprising:

a frame buffer receiving a substantially continuous video signal representing raw video content and dividing the data signal into individual frames which each store a fixed amount of data in digital form;

a processor generating a fixed-length original cryptographic hash from at least one such individual frame and encrypting the original cryptographic hash using an encryption cryptographic key selected from a cryptographic key pair; and

a recorder storing the encrypted original cryptographic hash as a digital signature on a transportable storage medium for retrieval and verification using a decryption cryptographic key selected from the cryptographic key pair; [[and]]

~~a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key such that a plurality of encryption cryptographic keys, each associated with a different removable storage medium, are capable of being utilized for encrypting the individual frames;~~

wherein the decryption cryptographic key is validated against user-provided credentials prior to decrypting the encrypted frames;

wherein a set of cryptographic instructions [[is stored on the removable storage medium and]]employs at least one of the encryption cryptographic key and the decryption cryptographic key;

wherein a removable storage medium stores at least one of the encryption cryptographic key or the decryption cryptographic key such that a plurality of encryption or decryption cryptographic keys, associated with the removable storage medium, are capable of being utilized for encrypting or decrypting the individual frames, where the removable storage medium comprises only memory that stores the set of cryptographic instructions and the plurality of the encryption or decryption cryptographic keys, and is separate from a player which is capable of playing the video content on the transportable storage medium or the recorder which is capable of recording the video content on the transportable storage medium;

wherein only encrypted and signed video content passes a first physical boundary separating [[a]]the recorder from the transportable storage medium;

wherein only the encrypted and signed video content passes a second physical boundary separating the transportable storage medium from [[a]]the player;

~~wherein only signed video content passes the first physical boundary separating the recorder from the transportable storage medium;~~

~~wherein only the signed video content passes the second physical boundary separating the transportable storage medium from the player~~.

Claim 60: A method for digitally signing private video content using embedded cryptographic security, comprising:

receiving a substantially continuous video signal representing raw video content and dividing the data signal into individual frames which each store a fixed amount of data in digital form;

generating a fixed-length original cryptographic hash from at least one such individual frame;

encrypting the original cryptographic hash using an encryption cryptographic key selected from a cryptographic key pair;

storing the encrypted original cryptographic hash as a digital signature on a transportable storage medium for retrieval and verification using a decryption cryptographic key selected from the cryptographic key pair;

~~providing at least one of the encryption cryptographic key and the decryption cryptographic key on a removable storage medium such that a plurality of encryption cryptographic keys, each associated with a different removable storage medium, are capable of being utilized for encrypting the individual frames;~~

validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames; [[and]]

including a set of cryptographic instructions employing at least one of the encryption cryptographic key and the decryption cryptographic key[[on the removable storage medium]]; and

storing on a removable storage medium at least one of the encryption cryptographic key or the decryption cryptographic key such that a plurality of encryption or decryption cryptographic keys, associated with the removable storage medium, are capable of being utilized for encrypting or decrypting the individual frames, wherein the removable storage medium comprises only memory that stores the set of cryptographic instructions and the plurality of the encryption or decryption cryptographic keys, and is separate from a player which is capable of playing the video content on the transportable storage medium or a recorder which is capable of recording the video content on the transportable storage medium;

wherein only encrypted and signed video content passes a first physical boundary separating [[a]]the recorder from the transportable storage medium;

wherein only the encrypted and signed video content passes a second physical boundary separating the transportable storage medium from [[a]]the player;

~~wherein only signed video content passes the first physical boundary separating the recorder from the transportable storage medium;~~

~~wherein only the signed video content passes the second physical boundary separating the transportable storage medium from the player~~.

Claim 64: A system for verifying digitally signed private video content using embedded cryptographic security, comprising:

a player retrieving a digital signature from a transportable storage medium, the digital signature containing an original cryptographic hash encrypted using an encryption cryptographic key selected from a cryptographic key pair; and

a processor decrypting the encrypted original cryptographic hash using a decryption cryptographic key selected from the cryptographic key pair, generating a verification fixed-length cryptographic hash from at least one individual frame retrieved from the transportable storage medium, and comparing the verification cryptographic hash and the original cryptographic hash;

~~a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key such that a plurality of encryption cryptographic keys, each associated with a different removable storage medium, are capable of being utilized for encrypting the at least one individual frame;~~

wherein the decryption cryptographic key is validated against user-provided credentials prior to decrypting the encrypted frames;

wherein a set of cryptographic instructions [[is stored on the removable storage medium and]]employs at least one of the encryption cryptographic key and the decryption cryptographic key;

wherein a removable storage medium stores at least one of the encryption cryptographic key or the decryption cryptographic key such that a plurality of encryption or decryption cryptographic keys, associated with the removable storage medium, are capable of being utilized for encrypting or decrypting the individual frames, where the removable storage medium comprises only memory that stores the set of cryptographic instructions and the plurality of the encryption or decryption cryptographic keys, and is separate from the player which is capable of playing the video content on the transportable storage medium or a recorder which is capable of recording the video content on the transportable storage medium;

wherein only encrypted and signed video content passes a first physical boundary separating [[a]]the recorder from the transportable storage medium;

wherein only the encrypted and signed video content passes a second physical boundary separating the transportable storage medium from [[a]]the player;

~~wherein only signed video content passes the first physical boundary separating the recorder from the transportable storage medium;~~

~~wherein only the signed video content passes the second physical boundary separating the transportable storage medium from the player~~.

Claim 67: A method for verifying digitally signed private video content using embedded cryptographic security, comprising:

retrieving a digital signature from a transportable storage medium, the digital signature containing an original cryptographic hash encrypted using an encryption cryptographic key selected from a cryptographic key pair;

decrypting the encrypted original cryptographic hash using a decryption cryptographic key selected from the cryptographic key pair;

generating a verification fixed-length cryptographic hash from at least one individual frame retrieved from the transportable storage medium and comparing the verification cryptographic hash and the original cryptographic hash;

~~providing at least one of the encryption cryptographic key and the decryption cryptographic key on a removable storage medium such that a plurality of encryption cryptographic keys, each associated with a different removable storage medium, are capable of being utilized for encrypting the at least one individual frame;~~

validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames; and

including a set of cryptographic instructions employing at least one of the encryption cryptographic key and the decryption cryptographic key[[on the removable storage medium]];

wherein a removable storage medium stores at least one of the encryption cryptographic key or the decryption cryptographic key such that a plurality of encryption or decryption cryptographic keys, associated with the removable storage medium, are capable of being utilized for encrypting or decrypting the individual frames, where the

removable storage medium comprises only memory that stores the set of cryptographic instructions and the plurality of the encryption or decryption cryptographic keys, and is separate from a player which is capable of playing the video content on the transportable storage medium or a recorder which is capable of recording the video content on the transportable storage medium;

wherein only encrypted and signed video content passes a first physical boundary separating [[a]]the recorder from the transportable storage medium;

wherein only the encrypted and signed video content passes a second physical boundary separating the transportable storage medium from [[a]]the player;

~~wherein only signed video content passes the first physical boundary separating the recorder from the transportable storage medium;~~

~~wherein only the signed video content passes the second physical boundary separating the transportable storage medium from the player~~.

Allowable Subject Matter

1. Claims *1, 3, 5-7, 10, 12, 14-16, 19, 20, 22-24, 26, 28-30, 32, 33, 35-37, 39, 42, 43, 45, 46, 48, 51, 53, 56-58, 60, 61, 63-65, 67 and 70* are allowed.

2. The following is an examiner's statement of reasons for allowance:

The above mentioned claims are allowable over prior arts because the CPA (Cited Prior Art) of record fails to teach or render obvious the claimed limitations in combination with the specific added limitations, as recited in all independent claims and subsequent dependent claims.

The prior arts Brothers, alone or in combination with Barton and Tsuria, fail to teach or suggest a system for automatically protecting private video content using

embedded cryptographic security that comprises a recorder frame buffer, an encryption module, a decryption module, a playback frame buffer, a signature module, a verification module, and a removable storage medium storing at least one of the encryption cryptographic key or the decryption cryptographic key such that a plurality of encryption or decryption cryptographic keys, associated with the removable storage medium, are capable of being utilized for encrypting or decrypting the individual frames, wherein the removable storage medium comprises only memory that stores the set of cryptographic instructions and the plurality of the encryption or decryption cryptographic keys, and is separate from a player which is capable of playing the video content on the transportable storage medium or a recorder which is capable of recording the video content on the transportable storage medium.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AVAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100